DIGITÁLNA BUDÚCNOSŤ

UNIMED Prešov: Dilema po Krádeži Zdravotných Záznamov

Prípadová štúdia o kybernetickom incidente vo fakultnej nemocnici – a rozhodnutí, ktoré formuje budúcnosť bezpečnosti pacientov.

PRÍPADOVÁ ŠTÚDIA Igor Straka

19.03.2026, Roadshow Digitálna budúcnosť, M Aréna Prešov

O Nemocnici

UNIMED Prešov — Fakultná nemocnica

Nemocnica s ~450 zamestnancami (lekári, sestry, administratíva) poskytujúca špecializovanú zdravotnú starostlivosť v Prešovskom regióne. Jej IT infraštruktúra zahŕňa rozsiahlu sieť IoMT zariadení – infúzne pumpy, monitory pacientov a systémy elektronických zdravotných záznamov (EZR).

~450

Zamestnancov

IoMT

Rozsiahla sieť medicínskych zariadení

EZR

Centrálny systém zdravotných záznamov

DIGITÁLNA BUDÚCNOSŤ

Priebeh Incidentu

Exploatácia

IoMT: predvolené heslá, nepatche

Laterálny pohyb

Presun do EHR cez kompromitované zariadenia

Exfiltrácia

7 200 záznamov: diagnózy, genetika

Únik

Údaje na dark webe na predaj

Útočník využil reťazec zraniteľností – od nepatchovaných IoMT zariadení s predvolenými heslami až po exfiltráciu citlivých zdravotných údajov osobitnej kategórie podľa GDPR čl. 9.

DIGITÁLNA BUDÚCNOSŤ

Rozsah Úniku a Bezprostredné Dopady

7 200

Zdravotných záznamov

Diagnózy, liečba, genetické a psychiatrické údaje

18h

Narušenie starostlivosti

Oneskorenie infúzií a monitoringu pacientov

4%

Hrozba pokuty GDPR

Až 4 % ročného obratu + NIS2 sankcie

Dáta osobitnej kategórie (psychiatrické záznamy, genetické údaje) podľa GDPR čl. 9 – najvyššia úroveň ochrany a zodpovednosti. Dáta sa objavili na dark webe a útočník ich aktívne ponúka na predaj.

DIGITÁLNA BUDÚCNOSŤ

Odhalené Kritické Slabiny

65 % IoMT zariadení

Má známe, zneužiteľné zraniteľnosti – legacy OS a firmware bez podpory aktualizácií.

Absencia MFA

Viacfaktorová autentifikácia chýba na väčšine administrátorských účtov pre medicínske systémy.

Žiadna sieťová segmentácia

IoMT zariadenia nie sú monitorované ani izolované – nulová viditeľnosť pohybu v sieti.

Slabý patch manažment

Priorita na klinickú funkčnosť – bezpečnostné aktualizácie zariadení systematicky zanedbávané.

DIGITÁLNA BUDÚCNOSŤ

KRITICKÁ DILEMA

Dve Cesty — Jedno Rozhodnutie

Možnosť A — Agresívne Posilnenie

Okamžité kroky:

- Segmentácia siete pre IoMT + povinné MFA
- Urgentný inventár a patch/upgrade kritických zariadení
- Kontinuálny monitoring + vulnerability scanning
- Externý audit NIS2/GDPR

Investícia: ~€180 - 250 tis. v roku 1

Riziko: Odpor personálu, pokles efektivity starostlivosti o 10 - 18 % počas prechodu

Možnosť B — Postupné Zavádzanie

Mäkký prístup:

- Pilot segmentácie len na vybraných oddeleniach (napr. JIS)
- Dobrovoľné školenia, postupný upgrade podľa rizikovosti
- Investícia najprv do lacnejších opatrení (inventár, awareness)

Riziko: Oneskorenie → ďalší incident môže byť katastrofálny – ďalšia exfiltrácia, vysoké pokuty GDPR/NIS2, trvalé reputačné škody

Porovnanie Rizík: Možnosť A vs. B

Kľúčová otázka

Nie je to len finančná kalkulácia – je to otázka **zodpovednosti voči pacientom** a regulačnej povinnosti. Ďalší incident s rovnakými koreňovými príčinami by bol pre regulátory dôkazom úmyselného zanedbania.

GDPR čl. 9 + NIS2: Nemocnica je povinná prijať "primerané technické a organizačné opatrenia". Nečinnosť po zdokumentovanom incidente zvyšuje právnu expozíciu.

Ako Získať Buy-in od Klinického Personálu?

Jazyk pacienta, nie IT

Komunikovať bezpečnosť ako ochranu pacienta: „MFA chráni vaše prístupové práva, aby nikto iný nemohol meniť príkazy pre infúzne pumpy."

Zapojiť lídrov oddelení

Primári a hlavné sestry ako ambasádori zmeny – nie IT tím vydávajúci príkazy, ale klinickí lídri obhajujúci bezpečnosť pacientov.

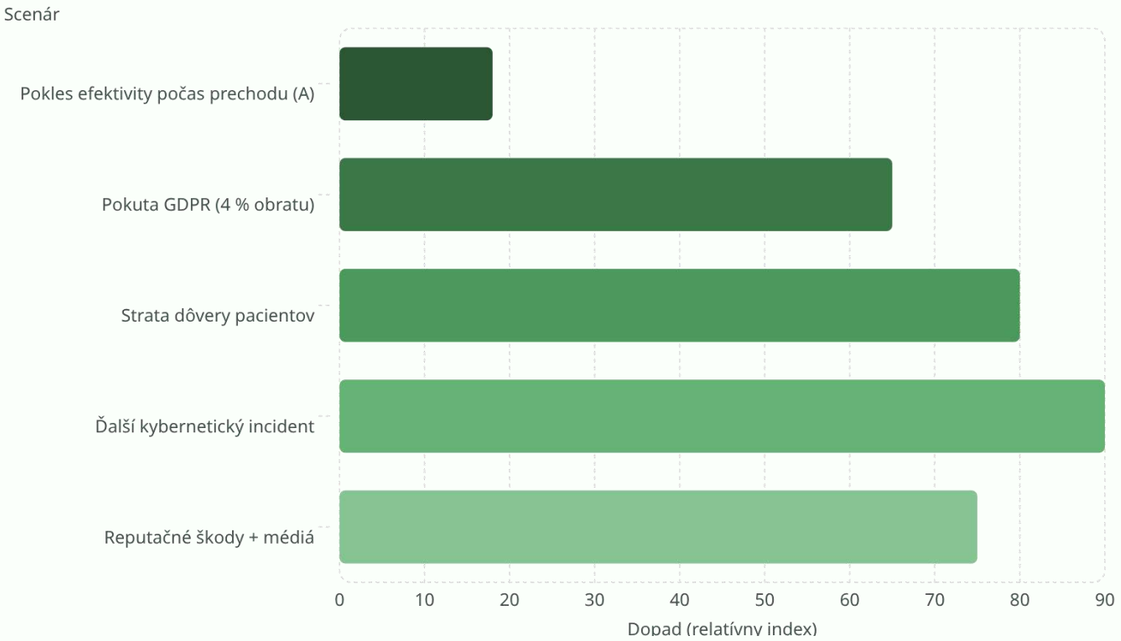
Piloty, nie revolúcia

Testovať zmeny najprv na dobrovoľníkoch z oddelení – zbierať spätnú väzbu a upravovať pred plošným zavedením.

Garantovať kontinuitu

Jasný protokol: v urgentnej situácii má klinická potreba vždy prednosť – bezpečnostné opatrenia nesmú blokovať záchranu života.

Krátkodobé vs. Dlhodobé Riziko

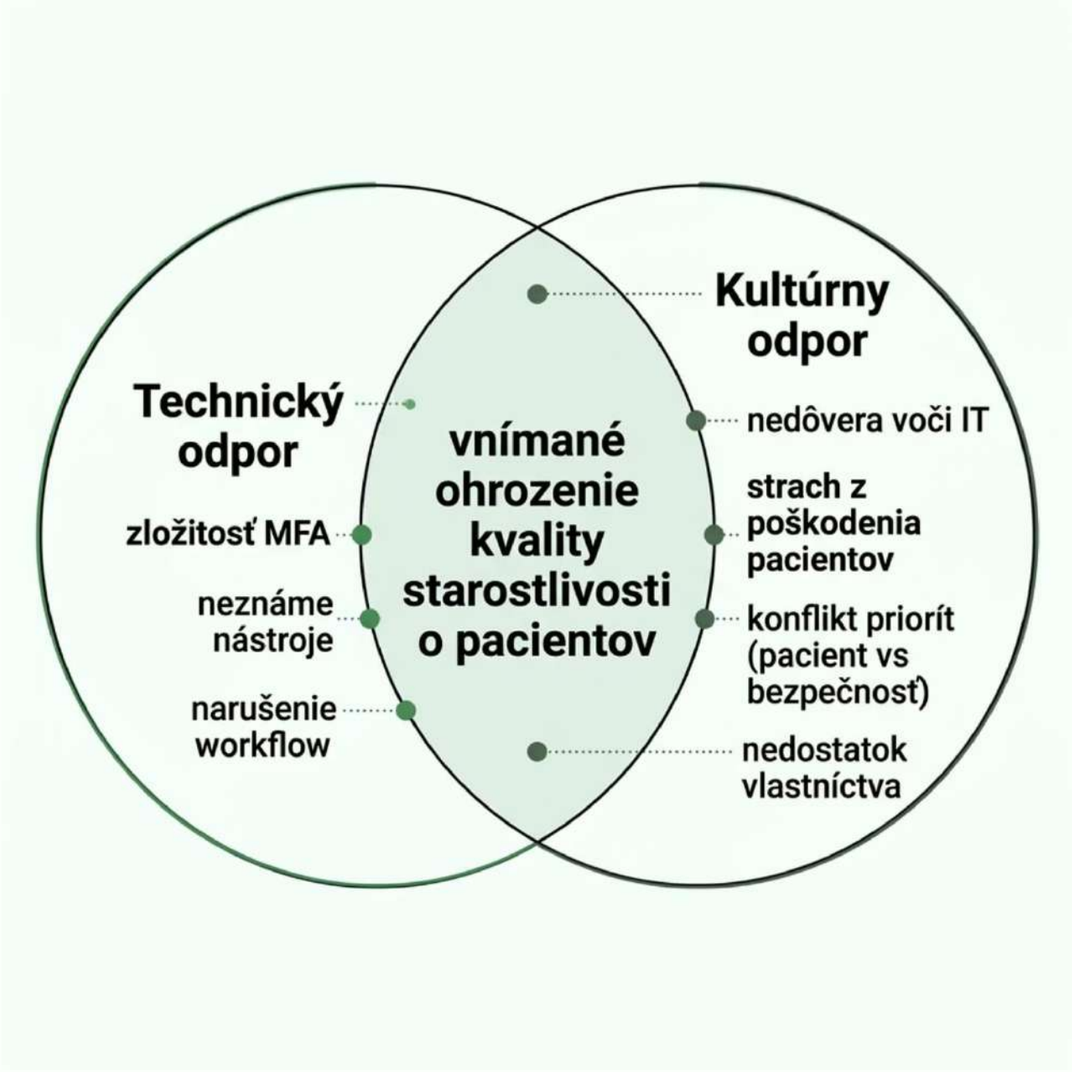


Interpretácia

Dočasný pokles efektivity pri zavádzaní Možnosti A je **rádovo menší** ako potenciálne dopady ďalšieho incidentu. Regulačné sankcie, strata dôvery pacientov a mediálny tlak môžu ohroziť samotnú prevádzku nemocnice.

Krátkodobá nepohodlnosť vs. existenčné riziko – voľba je zrejmá.

Je Odpor Personálu Technický alebo Kultúrny?



Diagnóza odporu

Výskumy v zdravotníctve konzistentne ukazujú: **primárnym zdrojom odporu je kultúra, nie technika.** Lekári a sestry nie sú proti bezpečnosti – sú proti tomu, čo vnímajú ako prekážku starostlivosti o pacienta.

Riešenie: zmeniť naratív z „IT compliance" na „bezpečnosť pacienta je aj kybernetická bezpečnosť".

DIGITÁLNA BUDÚCNOSŤ

Otázky pre Diskusiu

1

Možnosť A alebo B?

Ako by ste rozhodli ako riaditeľ/primár? Aké argumenty sú pre vás rozhodujúce?

2

Prvý krok

Čo by ste urobili ako úplne prvé – ešte pred investíciami a auditmi?

3

Prijateľné kompromisy

Aké kompromisy medzi bezpečnosťou a klinickou efektivitou sú reálne v nemocničnom prostredí?

4

Buy-in od personálu

Ako presvedčiť lekárov a sestry, pre ktorých je prioritou pacient – nie IT bezpečnosť?

Ďalšie Otázky pre Hĺbkovú Diskusiu

1

Kultúra vs. technika

Je odpor personálu voči MFA a segmentácii spôsobený technickou náročnosťou, alebo organizačnou kultúrou a strachom z ohrozenia starostlivosti?

2

Práca s obavami

Ako môže vedenie efektívne pracovať s obavami z odpojenia zariadení počas urgentných situácií?

3

Dlhodobá rovnováha

Ako vyvážiť krátkodobý pokles efektivity (10 - 18 %) s dlhodobým rizikom masovej straty dôvery pacientov a sankcií GDPR/NIS2?

4

Váš prvý krok do 14 dní

Aký jeden konkrétny malý krok viete urobiť vo svojej organizácii do 14 dní, aby ste znížili riziko podobného incidentu?

DIGITÁLNA BUDÚCNOSŤ

Záver: Bezpečnosť ako Súčasť Starostlivosti

> Kybernetická bezpečnosť v nemocnici nie je IT problém – je to klinický a etický záväzok voči každému pacientovi, ktorého dáta a liečba závisia od spoľahlivosti digitálnej infraštruktúry.

Regulačná realita

GDPR + NIS2 nie sú voliteľné – nečinnosť po zdokumentovanom incidente je právne neobhájiteľná

Kultúrna zmena

Technické riešenia zlyhajú bez organizačného buy-inu – ľudia sú prvou líniou obrany

Jeden krok dnes

Každá organizácia môže začať malým krokom – inventár, MFA na jednom systéme, jedno školenie

DIGITÁLNA BUDÚCNOSŤ

Prosím, naskenujte QR Kód pre hodnotenie aktivity.